U.S. Department of Justice

United States Attorney
Southern District of New York

The Silvio J. Mollo Building
One Saint Andrew's Plaza
New York, New York 10007

January 13, 2005

BY HAND

Honorable Alvin K. Hellerstein
United States District Judge
United States District Court
500 Pearl Street
New York, New York 10007

Re: United States v. Jason Smathers,
04 Cr. 1273 (AKH)
04 Cr. 1314 (AKH)

Dear Judge Hellerstein:

The Government respectfully submits this letter in connection with the anticipated guilty plea of defendant Jason Smathers, in order to provide the Court with certain information regarding the recently enacted Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (hereinafter, "CAN-SPAM Act"), and to set forth how Smathers agreed to violate that statute, and engaged in other criminal conduct as charged.

As explained below, Jason Smathers conspired to steal, and did steal, a highly valuable piece of intellectual property from America Online ("AOL"). Indeed, he stole one of AOL's most important business assets: its customer list, containing approximately 92 million internet screen names of AOL's customers worldwide. Smathers stole this list for multiple purposes. He stole the list to sell it (and he sold it), and Smathers stole it to enable himself and others to send massive amounts of unsolicited commercial e-mails, also known as "Spam." He also agreed with others to engage in deceptive practices to ensure that the Spam sent in connection with the stolen list reached its intended recipients, and would not be detected and filtered out by anti-Spam technology. Smathers also discussed with his conspirators the possibility of stealing an updated AOL customer list, and of using the list himself to send Spam. By doing so, Smathers committed the crimes of interstate transportation of stolen property, and conspiracy to engage in the interstate transportation of stolen property, and to violate the CAN-SPAM Act.

Smathers has informed the Government and the Court that he wishes to enter a plea of guilty to all of the charges in the two Informations referenced above. Information 04 Cr. 1314 charges Smathers with a substantive violation of interstate transportation of stolen

property, and does not implicate the CAN-SPAM Act. The conspiracy charge contained in Information 04 Cr. 1273, has, two objects: the interstate transportation of stolen property, and a violation of CAN-SPAM. Smathers has informed the Government that he is prepared to admit to both charged objectives of the conspiracy.

I. Background

A. Spam And Its Economic Costs

As the Court is aware, e-mail users are literally inundated with unsolicited commercial e-mails, known as Spam. Because many e-mail users do not wish to receive Spam, numerous commercial entities that provide e-mail service to their customers (called Internet Service Providers, or "ISPs") such as AOL, have engaged in extensive efforts to acquire technology to enable them to prevent Spam from reaching the electronic mailboxes of their customers. These anti-Spam measures are typically highly sophisticated technology that includes software, known as Spam filters, that identify computers that have previously sent Spam, and that block any additional e-mails sent from such computers from entering those customer mailboxes. ISPs actually compete with each other for customers by describing their investments in, and the success of, their anti-Spam technology, and the inclusion of such technology in a package of internet services is often used by ISPs to enhance the desirability of their services to customers, and are often touted in ISPs marketing efforts.

As a result of the efforts of the ISPs to filter out their unsolicited messages, Spammers have taken to deliberately disguising the source (i.e., the computer locations from which they are initiating their e-mailing operations) of their Spam. They do so for several reasons. Spammers seek to ensure that (a) the Spam they send actually reaches the target e-mail in-boxes, and is not filtered out or rejected by anti-Spam mechanisms, and (b) that the targeted recipients actually open and read the Spam e-mail, rather than reject it as coming from an unknown or unwanted source. To accomplish these goals, Spammers take various steps to hide the source of their messages in order to sneak their messages passed the highly sophisticated anti-Spam defenses of ISPs such as AOL, and to lure consumers into mistakenly opening messages that appear to be from people they know (or at least not from Spammers).

The Government has been informed by AOL that the transmission of Spam forces excessive numbers of e-mails into AOL's mail servers which, in turn, destabilizes the AOL network by reducing system reliability and efficiency. AOL's mail servers and Spam filters have a finite processing speed and memory storage capacity that limit AOL's ability to receive, sort, deliver, and store email and thus limit the rate at which email can be processed. Because Spammers can, as discussed below, disguise the origin of their messages, AOL's e-mail system must spend time processing e-mails to distinguish legitimate e-mail from Spam. AOL's network capacity is consumed as its mail servers and Spam filtering processes examine and sort millions of Spam messages that are disguised to look like legitimate e-mail.

Further, AOL's technical staff must continuously monitor the Spam transmitted to the AOL network and take action when Spam reaches AOL members. Because the transmission of Spam diverts valuable human, financial, and e-mail processing resources and consumes mail server capacity (among other harms), AOL is harmed by any and all unauthorized Spam. As a result of Spam, AOL has had to invest enormous sums of money to both handle the massive volume of incoming messages and filter out those that are unwanted Spam. Not only do ISPs like AOL bear the costs of Spamming: AOL members who pay telephone toll charges to access the Internet, or to access email on wireless devices, incur directs costs for receiving, reviewing, deleting, and trying to avoid future receipt of Spam.

The defining economic reality of Spam is that it is free to send, but costly to receive - both in terms of the preventative efforts of ISPs to stop Spam from reaching consumers, and in terms of customer goodwill when Spam (and its usually objectionable content) successfully evades ISP filters and reaches the consumer. Spammers force ISPs to bear the costs of processing, filtering, and addressing customer complaints caused by junk email advertisements. Congress recently found that Spam costs Internet subscribers $9.4 billion per year, and is likely to cost corporations over $113 billion by 2007. S. Rep. No. 108-102, at 6-7 (2003). Junk e-mail devours computer processing and storage capacity, slows down data transfer between computers over the Internet by congesting the electronic paths through which the messages travel, and causes recipients to spend time and money wading through messages they do not want.[1]

B. IP Addresses, Headers, and Proxies - Technological Methods Spammers Use to Disguise Themselves

IP Addresses: Computers connected to the Internet are identified by unique numeric addresses known as Internet Protocol (IP) addresses, e.g. 192.168.1.1. Because human beings find words easier to remember than numbers, a given IP address is normally associated with a specific name known as a "domain" name. For example, the domain name "nytimes.com" is associated with a specific IP address. When a user enters "nytimes.com" into the address bar of his Internet web browser, software on the user's machine "looks up" the IP address associated

[1] Through the deceptive act of disguising the origin of their Spam, Spammers effectively shift the costs of their advertising campaigns to the receiving ISPs. Open relays and proxies, which are described in more detail below, are important vehicles of Spammer "tradecraft" that help disguise Spam origin, and which allow Spammers to defeat the anti-Spam measures taken, at great cost by ISPs to prevent Spam from reaching recipients' inboxes. Those costs are then passed along by ISPs to consumers through higher monthly access fees. Moreover, as the Court recognized, some consumers become so fed up with Spam that they change ISPs. Still others may even lose trust in the integrity of e-mail as a communications medium, and may stop using e-mail entirely.

with that domain name, and connects to that IP address.

E-mail Headers: Many e-mail messages include information sufficient to identify the sender. This identifying information is contained in the "headers" of the e-mails. An e-mail "header" is a piece of machine-readable information attached by the computer to the e-mail message. Header information contains routing information that is often not seen or read by the human user and is used to direct the e-mail to the correct address. An e-mail program normally shows the user only the standard "To:," "From:," "Subject:," and "Date:" headers, but there are more header categories that are not always displayed to the human user. The IP address from which an e-mail has been sent is one of the pieces of information that is always in the header of an e-mail, whether that information is displayed to the human user or not. One common anti-Spam measure employed by ISPs is to look at the e-mail header information, including the IP address that sent the email, to determine whether the e-mail should be forwarded to the recipient.

One of the ways in which Spammers disguise their identities is by inserting deceptive header information in their e-mails -- that is, by altering the data within the e-mails that would otherwise correctly identify them (to ISPs and to e-mail recipients) as the true sender of those e-mail. More specifically, they frequently do so by intentionally routing and transmitting their masses of commercial e-mail through machines -- relays and proxies -- that altered the header information of the e-mails, with the intent that the header information will be altered as a result of the routing. This intentional routing mechanism is one method by which Spammers attempt to defeat the prophylactic measures taken by ISPs and e-mail recipients to filter and avoid Spam.

Open Proxies[2]: An open proxy is a computer server that accepts electronic

---

[2] An explanation of open relays and proxies is provided in the Federal Trade Commission's recent publication, National Do-Not-Email Registry, A Report to Congress, Federal Trade Commission, June 2004, available at http://www.ftc.gov/reports/dneregistry/report.pdf (last visited January 3, 2005) (hereafter "FTC Report, p. ___"). See also generally, Inside the SPAM Cartel, Posluns and "Spammer-X", Syngress (2004) (hereafter "SPAM Cartel, p. ___").

An "Open Relay" is a computer server that accepts connections from another other mail server and processes e-mail messages directed to any network attached to the Internet. FTC Report, p. 9. These open mail servers are configured, often by mistake, to accept and deliver e-mail on behalf of any user anywhere. FTC Report, p. 9-10. A Spammer who connects to a computer operating as an open relay can intentionally insert false header information, including a forged source IP address, into e-mail sent through that open relay. By processing mail that is neither for nor from an authorized user, an open relay makes it possible for an unscrupulous sender to route large volumes of Spam. SPAM Cartel, pp. 32-36.

transmissions of data from the Internet and repackages those transmissions, so that they appear to have originated solely from the computer server acting as a proxy. FTC Report, pp. 9-11. With respect to e-mails, using an open proxy alters the header information in the e-mails. That is, once the transmission passes through the proxy, the proxy's IP address, not the IP address of the Spammer, appears in the header as the source IP address of the e-mail. Once this change occurs, the Spammer can no longer be identified as the source of the Spam, and the Spammer essentially becomes invisible, both to the ISPs who receive and process the Spam, and by the end recipient of the Spam. Thus, Spammers use open proxies to send transmissions anonymously to other computers. By sending e-mails through these routes, once the transmission goes through the proxy, any mail that the Spammer sent now appears to have originated from that "proxy" mail server -- not from the Spammer's computer.

Spammers have learned that by hijacking computers that do not belong to them to act as proxies, they can "launder" their Spam, delivering their unsolicited e-mail while fraudulently concealing their identity to make their messages appear to come from a legitimate source. SPAM Cartel, p. 34-35, 41-43 (describing the "big business" of selling and renting proxies for Spamming). Among other things, Spammers who unlawfully use third-party proxies damage the reputation of those whose machines they have hijacked, clog networks with junk mail, and frequently crash servers from masses of Spam that is returned to those servers as "undeliverable."

Most open proxies that exist on the Internet are simply computers in companies or homes that have been illicitly reconfigured, without the knowledge or approval of their owners, to act as proxies. (These compromised machines are frequently referred to as a "zombie" or "bot" machines). These "zombie" machines have often been compromised by a computer "virus" or "worm," initiated by someone other than the machine's true owner. The virus inserts software that turns the computer into an open proxy. Once converted, the compromised zombie computer will then permit further unauthorized access to itself -- often by Spammers, who use it as a proxy for sending their illicit Spam. SPAM Cartel, pp. 41-43 (describing the rise of "BOTnets," networks of compromised computers used to send Spam). Thousands of compromised zombie machines are collected in large "bot" networks which are then sold or rented to Spammers for anonymously sending bulk e-mail. It is now estimated that zombie computers are the source of more than 70% of Spam worldwide.[3]

---

[3] ZDnet.uk, "Most Spam Generated by Botnets, says Expert," quoting Steve Linford of Spamhaus.org, a internationally recognized anti-Spam organization, available at http://news.zdnet.co.uk/internet/security/0,39020375,39167561,00.htm (last visited January 6, 2004). See also FTC Report, p. 10 describing the growing threat of botnets and noting that one U.S. ISP reported that 56% of all Spam sent to its subscribers was routed through proxies located outside the United States.

Moreover, proxies and relays make it more difficult, if not impossible, for ISPs to filter out, through the use of anti-Spam measures, the waves of commercial e-mails that their customers wish to avoid. Many types of anti-Spam measures are built to examine the header information contained in incoming electronic transmissions, and to identify the computer IP address from which the transmission is coming. This is akin to a border inspection officer standing in a port of entry, checking passports of persons who would seek to enter a country. That border inspector might have a list of names or countries, for which he is under instructions to refuse entry. Similarly, ISPs systems are configured to recognize certain IP addresses as likely sources of Spam, and to refuse to process electronic communications originating from those IP addresses. When Spammers send their Spam through open proxies, the altered e-mail headers achieved by that deceptive routing makes it more difficult for an ISP to discover that its system is under attack by a Spammer. ISPs take steps to identify, and "blacklist" the IP Addresses of servers that are used as proxies to route Spam, and then block e-mail traffic routed through those servers. However, the technological sophistication of the use of proxies and relays to disguise the origin of Spam will defeat an ISP's efforts to filter out Spam based on the source IP address.[4] Indeed, Spammers often mount their Spam attacks by routing them through many intermediate computers en route to the recipient ISP, to create confusion and to prolong the inability of the ISP to effectively defend against the Spam attack.

II. The Congressional Response

In light of the enormous financial costs posed to email users and ISPs by Spam, Congress enacted the CAN-SPAM Act.

The CAN-SPAM Act of 2003, codified at Title 18, United States Code, Section 1037, makes it a crime to perpetrate certain forms of mass e-mail marketing campaigns. In enacting the statute, Congress made the following findings:

> (1) Electronic mail has become an extremely important and popular means of communication, relied on by millions of Americans on a daily basis for personal and commercial purposes. Its low cost and global reach make it extremely convenient and

---

[4] The majority of illicit open proxies are installed illegally on computers belonging to home users attached to a broadband Internet connection. These computers become unwitting tools in the Spammers' proxy network, without the consent or authorization of the system owner. Among the various victims of Spammers who hijack other people's computers to use as proxies are these unwitting computer owners. Often those owners will find, to their chagrin, that their network or computer has been blacklisted, and thus unable effectively to use the internet, because ISPs have identified them as sources of Spam, even though those owners were never aware that someone else (the Spammers) were using their computers for this illicit purpose.

efficient, and offer unique opportunities for the development and growth of frictionless commerce.

(2) The convenience and efficiency of electronic mail are threatened by the extremely rapid growth in the volume of unsolicited commercial electronic mail. Unsolicited commercial electronic mail is currently estimated to account for over half of all electronic mail traffic, up from an estimated 7 percent in 2001, and the volume continues to rise. Most of these messages are fraudulent or deceptive in one or more respects.

(3) The receipt of unsolicited commercial electronic mail may result in costs to recipients who cannot refuse to accept such mail and who incur costs for the storage of such mail or for the time spent accessing, reviewing, and discarding such mail, or for both.

(4) The receipt of a large number of unwanted messages also decreases the convenience of electronic mail and crates a risk that wanted electronic mail messages, both commercial and noncommercial, will be lost, overlooked, or discarded amidst the larger volume of unwanted messages, thus reducing the reliability and usefulness of electronic mail to the recipient.

. . .

(6) The growth in unsolicited commercial electronic mail imposes significant monetary costs on providers of Internet access services, businesses, and educational and nonprofit institutions that carry and receive such mail, as there is a finite volume of mail that such providers, businesses, and institutions can handle without further investment in infrastructure.

(7) Many senders of unsolicited commercial electronic mail purposefully disguise the source of such mail.

. . .

(9) While some senders of bulk unsolicited commercial electronic mail messages provide simple and reliable ways for recipients to reject (or "opt out" of) receipt of commercial electronic mail from such senders in the future, other senders provide no such "opt out" mechanism, or refuse to honor the requests of recipients not to

> receive electronic mail from such senders in the future, or both.

CAN-SPAM Act, Pub. L. No. 108-187, § 2(a), 117 Stat. 2699-2700 (2003) (emphasis added).

> Based on these findings, Congress concluded that:
>
> (1) [T]here is a substantial government interest in regulation of commercial electronic mail on a nationwide basis;
>
> (2) senders of commercial electronic mail should not mislead recipients as to the source or content of such mail; and
>
> (3) recipients of commercial electronic mail have a right to decline to receive additional commercial electronic mail from the same source.

Id. at § 2(b), 117 Stat. at 2700 (emphasis added).

Based on these findings and conclusions, Congress decided to criminalize certain practices related to the transmission on unsolicited commercial e-mails. Significantly, Congress did not, of course, criminalize sending commercial e-mail, or even sending unsolicited commercial e-mail.[5] Rather, as is relevant to this case, Congress criminalized the sending of commercial e-mails that fraudulently or deceptively misidentify their true source -- i.e., Congress prohibited people from intentionally disguising the source of a commercial e-mail, in order to deceive the recipient of the e-mail or ISPs regarding the true sender of the email.

In enacting 18 U.S.C. § 1037, Congress intended to criminalize various types of deceptive methods typically used by Spammers to disguise the true sender of commercial e-mails. Thus, among other things, CAN-SPAM makes it a crime to

- "hack" into (i.e., enter without authorization) someone else's computer to use that as a base for sending masses of commercial e-mail (which among other things, would disguise the actual sender),

- send masses of commercial e-mail through "relays" or retransmission mechanisms with the intent thereby to disguise the source of such e-mail from recipients or Internet Service Providers ("ISPs") (such as AOL),

---

[5] The CAN-SPAM Act does, however, establish certain civil regulatory requirements for sending unsolicited commercial e-mail in bulk. See generally 15 U.S.C. § 7704 (a) (1) (prohibition of false or misleading transmission information).

- falsify header information in masses of commercial e-mails, or

- register multiple e-mail accounts or other computer-based locations, using false or fraudulent information that hides the identity of the registrant, and use those accounts to send masses of commercial e-mail.

See 18 U.S.C. § 1037(a)(1)-(5).

In this case, the specific provision of Section 1037 that Smathers is charged with agreeing to violate is 18 U.S.C. § 1037(a)(2), which states, in relevant part:

> Whoever, in or affecting interstate or foreign commerce, knowingly –
>
> > (2) uses a protected computer to relay or retransmit multiple commercial electronic mail messages, with the intent to deceive or mislead recipients, or any Internet access service, as to the origin of such messages,
> >
> > shall be punished as provided for in subsection (b).

As Congress has recognized, disguising the true origin of an email is deceptive and harmful for two distinct reasons. First, Spammers use certain retransmission tactics to sneak their commercial messages past the anti-Spam defenses of the ISP, and to avoid accountability for transmitting that Spam. Second, in seeking to conceal their identity, Spammers also hope to lure consumers into believing that the messages are legitimate commercial messages.

In enacting the CAN-SPAM Act, Congress therefore determined that commercial e-mail senders should not intentionally mislead recipients or service providers as to the source of bulk commercial electronic mail. Senate Report 108-170 notes that ISPs "are doing their best to shield customers from Spam blocking billions of unwanted e-mails each day, but the Spammers are winning the battle . . . [because a]mong the barriers ISPs face when attempting to stop Spam is that Spammers use false and fraudulent means to avoid detection and identification." S. Rep. 108-170 at 2 (2003) (emphasis added).[6] By the Act, Congress has simply told senders of

---

[6] Senate Report 108-170 is the Senate Judiciary Committee report on S. 1293, "The Criminal Spam Act of 2003." On the day this report was issued, the criminal provisions of S. 1293 were incorporated into S. 877, "The CAN-SPAM Act of 2003," and formed the core of the criminal provisions of the final Act. See 149 Cong. Rec. S13027-28 (October 22, 2003) (proposal of amendment number 1893); *Id.* at 13032 (adoption of amendment 1893 by

unsolicited, bulk commercial e-mail that they must accurately identify themselves.

The specific forms of deception described above, which relate to the fraudulent cloaking of the origination point of Spam, are among the acts that Section 1037(a)(2) of the CAN-SPAM Act prohibits. As Congress explicitly stated: header information is "considered materially misleading if it fails to identify accurately [the] computer used to initiate the message because the person initiating the message knowingly uses another . . . computer to relay or transmit the message for purposes of disguising its origin." 15 U.S.C. §7704 (a) (1) (C). Put simply, header information is materially misleading, and therefore illegal, if it does not accurately identify the computer that sent the message because the sender disguised the true source by knowingly using another computer to relay or transmit the message.

Two of the principal goals sought to be achieved by the CAN-SPAM Act are (1) making sure that senders of commercial electronic mail not mislead recipients as to the source of such mail; and (2) ensuring that recipients of commercial electronic mail have a right to decline to receive additional commercial electronic mail from the same source. CAN-SPAM Act, Pub. L. No. 108-187, § 2(b)(2)-(3), 117 Stat. 2700. Both those Congressional goals are directly frustrated by Spammers's intentional use of open relays or proxies to the source of the Spam e-mail. Proxies and relays prevent consumers from effectively "opting-out" of receiving future mailings, as permitted by the Act, because Spammers have misrepresented the origin of the bulk e-mail. Unwilling recipients of such e-mail are unable to identify a person to contact to exercise their right to "opt out," and are further prevented from reporting to authorities who the source of their unwanted Spam is.

Notably, in enacting CAN-SPAM, the deception that Congress sought to remedy was not the sale of fraudulent or deceptive products through e-mail advertising. That activity is already well-covered through existing Federal mail fraud (e.g., 18 U.S.C. § 1341) and wire fraud (e.g., 18 U.S.C. § 1343) statutes.

---

unanimous consent).

III. Smathers' Criminal Conduct

The Government's investigation in this case has revealed the following information.[7]

Jason Smathers, a resident of Harpers Ferry, West Virginia, was an employee of AOL from 1999 up until June 23, 2003 -- the day he was arrested by Federal law enforcement authorities. For the latter part of Smathers' tenure at AOL, including the relevant time period, Smathers was employed as a software engineer, working at AOL's Dulles, Virginia, offices.

In April and May 2003, Jason Smathers entered into an agreement with other individuals to steal AOL's proprietary customer e-mail account database. This list, derived from years and multiple-millions of dollars worth of financial and labor investment, contained, among other information, screen names, account numbers, zip codes, credit card types (but no actual credit card numbers), and telephone numbers for all 30 million of AOL's worldwide customers.

While valuable to AOL in many ways, the primary value that AOL's customer list had for Smathers and his co-conspirators was for sending Spam. Indeed, it is difficult to overestimate the value of an e-mail list consisting of 92 million valid, current e-mail addresses to internet marketers who use such lists to flood recipients with their electronic marketing pitches for various products and services of dubious value.

Electronic communications recovered from Smathers's computer reflect his intent to use the list (and to provide it to others) to send Spam. In addition, Smathers believed, at that time, that it was wrong and illegal for him to take the list and use it for this purpose. Indeed, in the electronic discussion found on his computer, Smathers initially stated that Spamming AOL members is illegal, and he and the co-conspirator with whom he was then communicating went on to discuss various techniques by which to Spam AOL's customers. They also discussed the large profits to be made from such activity. At one point in the electronic discussion recovered from Smathers's computer, Smathers's co-conspirator wrote:

> Well . . . it would be different if you mailed current AOL members
> But the lists I use, and others have used, are just collected lists
> where people have to enter their emails and all there is thousands

[7] A copy of the Amended Criminal Complaint filed in this case is annexed hereto for the Court's convenience.

> and thousands of fake emails[8] If you have a database of REAL emails, that were fresh, the ratio of sign ups would be sooo much greater If you have any ideas on bulk mailing with AOL lol[9] let me know and I can get you a program set up in a heart beat heh"

Recognizing the need to conceal the nature of their illegal Spam activity, Smathers replied to this communication by stating:

> well I'll check it out . . . It isn't going to be easy I think I found the member database . . . Just need to figure out how to get the SNs [screen names] it is spread over like 30 computers . . . You can't talk about this. (Emphasis added).

As an insider at AOL, of course, Smathers was in a unique position to steal the customer list. Yet as he began his endeavor to assemble and remove a copy of AOL's entire customer list, the sheer vastness of the amount of data he was attempting to steal became apparent to him. Thus, for example, Smathers wrote to a co-conspirator:

> OK, I got it figured out . . . there are going to be millions of them so, will take time to extract I will do them a chunk at a time . . . because 37 million accounts have up to 7 screen names per account I'd expect there to be around 100 million active screen names maybe more.

In May 2003, Smathers, without authorization and using an employee access code assigned to another AOL employee, successfully extracted the complete list from AOL's proprietary data repository located in Virginia (the "Data Warehouse"), and delivered it to his co-conspirators. One Smathers's co-conspirators (referred to in Information 04 Cr. 1273 as "CC-1"), who resided in Nevada was, as Smathers was well aware, a professional internet marketer, who intended to use the list to send Spam promoting his internet gambling business.

---

[8] Lists of valid, working e-mail addresses useful for internet marketers (legitimate or illegitimate) are available in the marketplace, but they are not cheap. Companies often charge $500 for a list of 1000 e-mail addresses. However, such legitimate lists expire rapidly and therefore diminish in value to Spammers, because internet service customers change e-mail addresses frequently, and because once a list begins to contain too many invalid e-mail addresses, Spam filtering software used by Internet service providers begins to block all mail using such lists. The Government is informed that there are no legitimate e-mail lists for sale in the legitimate marketplace that contain 92 million valid, current e-mail addresses.

[9] In internet parlance, "lol" means "laughing out loud".

Shortly thereafter, CC-1 passed the list along to another co-conspirator (referred to in Information 04 Cr. 1273 as "CC-2"). CC-2, a professional internet marketer of, among other things, herbal penile enlargement pills, paid approximately $52,000 for the list. Smathers received thousands of dollars for performing his role in stealing the list, and also kept a copy of the list for his own use.

During the course of the conspiracy, CC-2 informed CC-1 of the nature his (CC-2's) Spamming business, including the fact that CC-2 employed the use of open proxies to perpetrate these mass e-mailings. As discussed above, this method of sending masses of commercial e-mail is one of the types of conduct that the CAN-SPAM Act defines as criminal, because it intentionally disguises the send of bulk, commercial e-mail. Further, CC-2 asked CC-1 to assist CC-2 in marketing CC-1's internet gambling business, by having CC-2 send out for CC-1 Spam promoting CC-1's business.

CC-2 and his business partner used the list, well into 2004, to Spam AOL's members, thereby flooding AOL's e-mail servers with literally billions of unsolicited, unwanted commercial e-mails that, because they were routed through proxy servers that cloaked the identity of their senders, violated CAN-SPAM, and caused AOL and its users damage. Indeed, CC-2 and his partner used several different mailing software products, including those known as "Super Mailer," "Proxy Hunter," "Aureate," and "Send Safe," to send these mailings through computers known as "open relays" or "open proxies" in order to deceive AOL about the true identity of the sender of the messages, to escape detection and liability for their unsolicited mailings.

Smathers membership in the conspiracy did not end with his delivery of the list to his co-conspirators. Indeed, Smathers continued for some time to discuss with his co-conspirators the potentially profitable uses of the list to him. Smathers also discussed with a co-conspirator a computer Spamming program he (Smathers) might use to take advantage of identity-concealing proxies servers, and the possibility that he himself might successfully take full advantage the list, for his own nascent marketing intentions, by using proxies in this way. Further, in 2004, the members of the Smathers's conspiracy discussed the possibility of Smathers stealing an updated AOL customer list.

IV. Discussion

The deceptive conduct criminalized by the CAN-SPAM act relates to the method of sending bulk, commercial e-mail, not the contents of the message intended to be read by the end recipient. The use of open proxies is deceptive and prohibited by the CAN-SPAM Act, because it aids Spammers to disguise themselves and the origin of their Spam, and thus enables them to successfully deliver their Spam, despite peoples' express desires to avoid it, and the ISPs

substantial investment in technological endeavors to block it.[10]

Put simply, computer users' rights not to receive unwanted commercial e-mail, and ISP's rights to avoid having to spend millions of dollars on technological filtering systems, are frustrated simply by the successful arrival of Spam e-mails into e-mail boxes. What Congress has recognized is that once the unwanted e-mails have arrived, the damage in terms of wasted resources is complete, whether or not the content of the e-mail contains any misrepresentations.[11]

By misrepresenting the origin of their bulk e-mail, Spammers impose the substantial costs of their business on consumers and ISPs and frustrate the CAN-SPAM Act's laudable goal of introducing authentication and accountability into commercial e-mail messages. Unchecked, these costs will continually increase, as Spammers and ISPs engage in an "arms race" of anti-Spam technologies and Spammers' circumvent countermeasures. Accordingly, the criminal prohibition in section 1037 (a)(2), which specifically prohibits re-transmitting and relaying e-mail messages in ways that intentionally disguise the sender, is an important provision that seeks to achieve Congress's objectives. Congress understood that criminal penalties were necessary to prevent Spammers from using deceptive tricks designed to hide the origin of Spam messages.

Based the undisputed facts of this case, Smathers is guilty of both counts for which he is charged, and the Court should accept the guilty plea accordingly, without reservation.

In order to prove the defendant guilty of the charge of Conspiracy in violation of 18 U.S.C. § 371 contained in 04 Cr. 1273, the Government would be required to prove the following at trial:

> First, that two or more persons entered the unlawful agreement charged in the Information;

---

[10] There is no serious question that Spam imposes significant economic burdens on ISPs, consumers, and businesses. Massive volumes of Spam can clog a computer network, slowing Internet service for those who share that network. ISPs must respond to rising volumes of Spam by investing at significant expense in new equipment to increase capacity and customer service personnel to deal with increased subscriber complaints. ISPs also face high costs maintaining e-mail filtering systems and other anti-Spam technology on their networks to reduce the deluge of Spam. And ISPs incur substantial costs of operation, simply because their systems are required to process millions, if not billions, of unwanted e-mail.

[11] Notably, Section 1037(a)(2) contains no "scheme to defraud" requirement. Rather, it is a "truthful identification" statute. Cf. 18 U.S.C. § 1028.

> Second, that Jason Smathers knowingly and willfully became a member of that conspiracy; and
>
> Third, that any of the co-conspirators -- not necessarily Smathers, but any one of the parties involved in the conspiracy -- knowingly committed at least one overt act in furtherance of the conspiracy during the life of the conspiracy.

That Conspiracy is further alleged to have had two objectives: (1) to commit interstate transportation of stolen property, in violation of 18 U.S.C. § 2314, and (2) to violate section 1037(a)(2) of the CAN-SPAM Act.

With respect to the first alleged objective, the elements of the crime of Interstate transportation of stolen property, 18, United States Code, section 2314 are:

> First, that goods, wares, merchandise, securities or money were stolen, converted or taken by fraud.
>
> Second, that a member of the conspiracy transported, transmitted or transferred (or caused to be transported or transmitted) the property in interstate or foreign commerce;
>
> Third, that at the time of the transportation or transmission, the defendant knew the property was stolen, converted or taken by fraud; and
>
> Fourth, that the value of the property was $ 5,000 or more.

Smathers plainly committed this crime. He entered into an agreement with others to steal, and did steal, the customer list of his employer, AOL. He sent that stolen property across State lines, and was paid thousands of dollars for doing so. The value of the stolen property was far in excess of $5,000, and at least one co-conspirator paid in excess of $52,000 for it. Thus, Smathers engaged in the interstate transportation of stolen property, and agreed with others to do so.[12]

With respect to the second objective of the conspiracy, the elements of a violation of the CAN-SPAM Act, subsection 18 U.S.C. § 1037(a)(2), (b)(2)(C) and (E) are:

---

[12] To the extent there might be any issue with respect to venue in this case, Smathers' plea agreement expressly provides he is waiving any venue challenges.

> First, that a co-conspirator knowingly used a protected computer[13] to relay or retransmit multiple[14] commercial e-mail messages;
>
> Second, that the co-conspirators caused the transmission with the intent to deceive or mislead recipients, or an Internet access service, as to the origin of such messages; and
>
> For purposes of triggering the felony provisions of the statute, EITHER
>
> Third, that the volume of e-mails transmitted in furtherance of the offense exceeded 2,500 in one day, or 25,000 over a 30-day period, or 250,000 over a one-year period
>
> OR
>
> Third, as a result of the offense the individuals committing the offense obtained thing of value in excess of $5,000 during 1-year period.

Smathers plainly agreed to commit this offense as well. He and his co-conspirators used the stolen AOL customer list for almost a year to send billions of Spam e-mails, and Smathers discussed personally using the list himself to send a high volume of commercial e-mails.[15] The volume of Spam sent by the co-conspirators far exceeded 250,000 e-mails in a one year period (indeed, a single mailing included millions of e-mails), and they reaped profits therefrom well in excess of $5,000 during that time period. The co-conspirators intended to, and did, send their Spam through open proxies to exploit proxies' identity-hiding

---

[13] For these purposes, a "protected computer" essentially includes any computer connected to the Internet.

[14] For these purposes, "multiple" is defined in 18 U.S.C. § 1037(d)(3) as in excess of 1,000 in one day, or 10,000 over a 30-day period, or 100,000 over a one-year period.

[15] The CAN-SPAM Act became effective January 1, 2004. The fact that Smathers' conspiracy commenced before that date does not present any ex post facto issue. See, e.g., United States v. Monaco, 194 F.3d 381, 386-87 (2d Cir. 1999) (noting that "[i]t is well settled that when a statute is concerned with a continuing offense [such as conspiracy], the Ex Post Facto clause is not violated by application of a statute to an enterprise that began prior to, but continued after, the effective date of the statute," and affirming conviction where money laundering conspiracy straddled enactment date of statute, despite admission of evidence of pre-enactment conduct at trial.) (quoting United States v. Harris, 79 F.3d 223, 229 (2d Cir.1996)).

properties, in order to make their Spamming more effective. It is these intentionally deceptive acts that are prohibited by the CAN-SPAM Act.

The damages caused to AOL as a result of Smathers's conspiracy are multifaceted and financially real. While some forms of damage to AOL -- such as damage to AOL's corporate goodwill and reputation, loss of customers who may have cancelled their subscriptions due to perceived security lapses or because of the quantity of Spam that may have escaped AOL's filters and arrived in the user's inbox -- may be difficult to measure, other forms of damage are known, and concretely measurable. In addition, AOL received 130,000 member complaints about the Smathers conspirators' Spam in the first six weeks of 2004 alone.

In this case, Jason Smathers, stands ready to admit he committed the crimes with which he is charged, and the parties have reached an agreement as to how to appropriately measure the damage caused by Smathers's crime. The parties have agreed that the appropriate measure is the costs incurred by AOL when it was forced, as a result of Smathers theft of its customer list, to process the billions and billions of unwanted e-mails sent to AOL users by the members of the conspiracy who used the list to frustrate AOL's anti-Spam technology and the send Spam to its customers.[16]

Smathers is therefore guilty of conspiring to perpetrate the type of deceptive conduct proscribed by the CAN-SPAM Act, including agreeing to disguise the origin of e-mail messages in an effort to see them delivered to the AOL customers.

The Government urges the Court to accept his plea.

Respectfully,

DAVID N. KELLEY
United States Attorney

By: _____
David M. Siegal
Assistant United States Attorney
(212) 637-2281

cc: John L. Pollok, Esq. (By fax and First Class mail)

[16] The Court should note that the measure of damage caused to AOL is not increased by the inclusion of the Section 1037 violation. The measure of damage would be the same were the defendant convicted solely of trafficking in stolen property and conspiring to do only that.